

REMARKS

This is a full and timely response to the non-final Office Action of August 4, 2004.

Reexamination, reconsideration, and allowance of the application and all presently pending claims are respectfully requested.

Upon entry of this First Response, claims 1-24 are pending in this application. The specification and claims 1 and 8-10 are directly amended herein, and claims 11-24 are newly added. It is believed that the foregoing amendments add no new matter to the present application.

Response to §112 Rejections

Claims 1-4 presently stand rejected under 35 U.S.C. §112, second paragraph, as allegedly failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. In this regard, it is alleged in the Office Action that the phrase “modified security settings” in claim 1 causes confusion. While Applicants disagree with the Examiner’s assessment, Applicants have amended claim 1 to remove the term “modified” in an effort to comply with the Examiner’s interpretation of the requirements set forth in the Office Action. Accordingly, the rejections to claims 1-4 under 35 U.S.C. §112 should be withdrawn.

Response to §102 and §103 Rejections

A proper rejection of a claim under 35 U.S.C. §102 requires that a single prior art reference disclose each element of the claim. See, e.g., *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 U.S.P.Q. 303, 313 (Fed. Cir. 1983).

Claim 1

Claim 1 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Pereira* (U.S. Patent No. 5,809,230). Claim 1, as amended, reads as follows:

1. A computer system, comprising:
memory;
a security application configured display a list of security rules to a user and to enable ones of said security rules based on user inputs, said security application configured to lock down resources of said computer system by modifying security settings of said computer system based on which of said security rules are enabled when an activation request is received by said computer system, ***said security application configured to store, in said memory, data indicative of said security settings, said security application configured to perform comparisons between said data and said security settings and to determine when one of said security settings has changed from a first value to another value based on one of said comparisons, said security application further configured to change said one security setting to said first value in response to said one comparison.*** (Emphasis added).

Applicants respectfully assert that the cited art fails to disclose at least the features of claim 1 highlighted hereinabove. Thus, the 35 U.S.C. §102 rejection of claim 1, as amended, is improper.

In this regard, it is asserted in the Office Action that *Pereira* teaches “said security application configured to store, in said memory, data indicative of said modified security settings (column 10, lines 10-13).” Thus, it is apparently alleged in the Office Action that the data stored in the “registry file” of *Pereira* constitutes the “data” recited by claim 1. It is further alleged in the Office Action that:

“said security application configured to perform comparisons between said data and said security settings and to determine when one of said security settings has changed from a first value to another value based on once of said comparisons, said security application further configured to change said one security setting to said first value in response to said one comparison (column 10, lines 64-column 11, line 6).”

The cited section of *Pereira* appears to describe an “access control program” that restricts the use of resources within a computer system. Thus, it is apparently the position of the Patent Office that

the “access control program” constitutes a “security application” that changes a “security setting” of a computer system when it detects a change of the “security setting” from a “first value to another value.” However, there is nothing in *Pereira* to indicate that such a “security setting” change is detected based on a comparison between the alleged “data” of the registry file and the alleged “security setting.” Indeed, there is nothing in *Pereira* to indicate that the detection of the alleged “security setting” change described at column 10 line 64, through column 11, line 6, is in any way based on the alleged “data” stored in the “registry file.” Accordingly, Applicants respectfully assert that *Pereira* fails to disclose “said security application configured to perform ***comparisons between said data and said security settings*** and to determine when one of said security settings has changed from a first value to another value ***based on one of said comparisons***, said security application further configured to change said one security setting to said first value ***in response to said one comparison***,” as recited by claim 1. (Emphasis added).

For at least the above reasons, Applicants respectfully asserts that *Pereira* fails to disclose each feature of claim 1. Accordingly, the 35 U.S.C. §102 rejection of claim 1 should be withdrawn.

Claims 2-4 and 11-17

Claim 2 presently stands rejected in the Office Action under 35 U.S.C. §103 as purportedly unpatentable over *Pereira* in view of *Proctor* (U.S. Patent No. 6,530,024). Further claims 3 and 4 presently stand rejected in the Office Action under 35 U.S.C. §102 as allegedly anticipated by *Pereira*. In addition, claims 11-17 have been newly added via the amendments set forth herein. Applicants submit that the pending dependent claims 2-4 and 11-17 contain all features of their respective independent claim 1. Since claim 1 should be allowed, as argued hereinabove, pending

dependent claims 2-4 and 11-17 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

Claim 5

Claim 5 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Pereira*.

Claim 5, as amended, reads as follows:

5. A computer system, comprising:
means for receiving a request for activating a security profile;
means for modifying security settings of a computer system in response to said request;
means for storing data indicative of said modified security settings;
means for automatically determining when one of said security settings has changed from a first value to another value ***by periodically comparing said data to said security settings***;
means for automatically changing said one security setting to said first value in response to a determination by said determining means that said one security setting has changed. (Emphasis added).

For at least the reasons set forth hereinabove in the arguments for allowance of claim 1, Applicants respectfully submit that the cited art fails to disclose at least the features of claim 5 highlighted above. Accordingly, the 35 U.S.C. §102 rejection of claim 5 should be withdrawn.

Claims 6, 7, and 18

Claim 6 presently stands rejected in the Office Action under 35 U.S.C. §103 as purportedly unpatentable over *Pereira* in view of *Proctor*. Further, claim 7 presently stands rejected in the Office Action under 35 U.S.C. §102 as allegedly anticipated by *Pereira*, and claim 18 has been newly added via the amendments set forth herein. Applicants submit that the pending dependent claims 6, 7, and 18 contain all features of their respective independent claim 5. Since claim 5 should be allowed, as argued hereinabove, pending dependent claims 6, 7, and 18 should be

allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

Claim 8

Claim 8 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Pereira*.

Claim 8, as amended, reads as follows:

8. A method for locking down resources of computer systems, comprising:
receiving a request for activating a security profile;
modifying security settings of a computer system in response to said
request;
storing data indicative of said security settings, as modified by said
modifying;
automatically determining when one of said security settings has changed
from a first value to another value ***by periodically comparing said data to said
security settings***; and
automatically changing said one security setting to said first value in
response to a determination in said determining that said one security setting has
changed. (Emphasis added).

For at least the reasons set forth hereinabove in the arguments for allowance of claim 1, Applicants respectfully submit that the cited art fails to disclose at least the features of claim 8 highlighted above. Accordingly, the 35 U.S.C. §102 rejection of claim 8 should be withdrawn.

Claims 9, 10, and 19

Claim 9 presently stands rejected in the Office Action under 35 U.S.C. §103 as purportedly unpatentable over *Pereira* in view of *Proctor*. Further, claim 10 presently stands rejected in the Office Action under 35 U.S.C. §102 as allegedly anticipated by *Pereira*, and claim 19 has been newly added via the amendments set forth herein. Applicants submit that the pending dependent claims 9, 10, and 19 contain all features of their respective independent claim 8. Since claim 8 should be allowed, as argued hereinabove, pending dependent claims 9, 10, and 19 should be

allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

Claim 20

Claim 20 has been newly added via the amendments set forth herein. Claim 20 presently reads as follows:

20. A computer system, comprising:
memory;
an operating system configured to analyze a machine state to control operation of said computer system, said machine state including a security setting associated with a resource of said computer system and indicating whether access to said resource is restricted, wherein said operating system is configured to analyze said security setting to control access to said resource; and
a security application configured to modify said security setting based on a user input and to store, in said memory, data indicative of a state of said security setting, as modified by said security application, said security application configured to perform a comparison between said data and said security setting to detect an unauthorized change of said security setting, said security application further configured to automatically change said security setting based on said data in response to a detection of an unauthorized change of said security setting.

Applicants respectfully submit that the cited art fails to disclose or teach each of the above features of pending claim 20. Accordingly, claim 20 is allowable.

Claims 21-24

Claims 21-24 have been newly added via the amendments set forth herein. Applicants submit that the pending dependent claims 21-24 contain all features of their respective independent claim 20. Since claim 20 should be allowed, as argued hereinabove, pending dependent claims 21-24 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

CONCLUSION

Applicants respectfully request that all outstanding objections and rejections be withdrawn and that this application and all presently pending claims be allowed to issue. If the Examiner has any questions or comments regarding Applicants' response, the Examiner is encouraged to telephone Applicants' undersigned counsel.

Respectfully submitted,

**THOMAS, KAYDEN, HORSTEMEYER
& RISLEY, L.L.P.**

By:



Jon E. Holland

Reg. No. 41,077

(256) 704-3900 Ext. 103

Hewlett-Packard Development Company, L.P.
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400